Notice of Allowability	Application No.	Applicant(s)	
	09/492,534	FRANKEL ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the response filed on 24 July 2006*.

2. ☒ The allowed claim(s) is/are *1 and 4-48*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the response filed on 24 July 2006.

2. Claims 1, 4-7, 24, 43 and 46 are amended by Examiner's Amendment below.

3. Claims 2 and 3 have been cancelled by Examiner's Amendment below.

4. Claims 1 and 4-48 are currently pending and have been examined.

Allowable Subject Matter

5. Claims 1 and 4-48 are allowed. See Reasons for Allowance under separate heading.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

7. Authorization for this examiner's amendment was given in a telephone interview with Jean Paul Hoffman on 20 July 2006.

8. The application has been amended as follows:

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) In an infrastructure in which some of a plurality of entities provide cryptographically supported services, a method of registering a subscriber entity of a plurality of entities at a principal entity of a plurality of entities, the method comprising:

the subscriber entity requesting service from the principal entity by sending a request message to a registrar entity of the plurality of entities;

the registrar entity verifying the subscriber entity and forwarding the request for service to the principal entity;

the principal entity storing the forwarded request and transmitting an acknowledgement message to the registrar entity, the acknowledgement stating acceptance and authentication/authorization information that the subscriber entity requires to obtain or access the requested service; and

the registrar entity verifying the authenticity of the received acknowledgement message, and, if correct, forwarding the acknowledgement message to the subscriber entity,

wherein the request message contains an indication of a type of service requested by the subscriber entity and contains one or more selected from the following:

(a) a unique reference to the subscriber entity;

(b) attributes about the subscriber entity;

(c) authentication information to be used to authenticate use of the service;

(d) transactional verification information;

(e) a representation by the subscriber entity agreeing to what the subscriber entity accepts;

(f) a preferred service relationship; or

(g) a subscriber entity's authenticator.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) A method as in claim 1~~3~~ wherein the unique reference to the subscriber entity is at least one selected from ~~of~~ (a) the subscriber entity's identity, (b) a pseudonym for one-time service, or ~~and~~ (c) a pseudonym for continued use of the service

5. (Currently Amended) A method as in claim 1~~3~~ wherein a session identifier links future responses to this particular request.

6. (Currently Amended) A method as in claim 1~~3~~ wherein the attributes about the subscriber entity include:

(a) a self-representation; and

(b) a third-party representation asserting attributes.

7. (Currently Amended) A method as in claim 6 wherein said representation and attribute include at least some selected from ~~of~~:

(a) an address;

(b) employment information;

(c) information from one or more other entities needed for service provisioning; or ~~and~~

(d) an authorization from another party.

8. (Original) A method as in claim 1 further comprising:

modifying the registration of the subscriber entity at the principal entity.

9. (Original) A method as in claim 1 further comprising:

moving the registration for service from the principal entity to another entity of said plurality of entities.

10. (Previously Presented) A method as in claim 1 wherein the service includes:

operating a cryptographically-supported transaction involving the subscriber entity, the principal entity and possibly one or more additional entities.

11. (Original) A method as in claim 1 wherein the subscriber entity comprises a plurality of elements.

12. (Original) A method as in claim 11 wherein the plurality of elements are associated with an entity.

13. (Previously Presented) A method as in claim 1 wherein said service is a subset of a totality of services.

14. (Previously Presented) A method as in claim 1 wherein said service is a warranty service.

15. (Previously Presented) A method as in claim 13 wherein another subset of the totality of services to the subscriber entity is provided by an entity different from the principal entity.

16. (Original) A method as in claim 15 wherein the subscriber entity can modify the subset of totality of services between entities.

17. (Previously Presented) A method as in claim 8 wherein modification is supervised by one or more authorities.

18. (Previously Presented) A method as in claim 9 wherein moving of services is supervised by one or more authorities.

19. (Previously Presented) A method as in claim 1 wherein provision of service may involve an additional entity from said plurality of entities.

20. (Previously Presented) A method as in claim 19 wherein provision of service is split between said principal entity and said additional entity.

21. (Original) A method as in claim 1 wherein provision of service by said principal entity on behalf of said subscriber entity is given by said operating infrastructure to an entity within said plurality of entities.

22. (Original) A method as in claim 1 wherein said provision of service by said principal entity involves other entities within said plurality of entities.

23. (Original) A method as in claim 14 wherein said warranty service involves correctness of representation of information.

24. (Currently Amended) A method as in claim 23 wherein said representation of information is at least one selected from ~~of~~: (a) identity information, (b) financial information; or ~~and~~ (c) information derived from provision of service within said infrastructure.

25. (Previously Presented) A method as in claim 14 wherein the infrastructure includes a mechanism to initiate claims against failed warranty.

26. (Previously Presented) A method as in claim 1 wherein provision of service involves control of access.

27. (Original) A method as in claim 1 wherein at least one of said plurality of entities is an enterprise.

28. (Original) A method as in claim 1 wherein at least one of said plurality of entities is a financial institute.

29. (Original) A method as in claim 1 wherein said principal entity is a group of elementary entities.

30. (Previously Presented) A method as in claim 1 wherein provision of service by said principal entity is directed by said subscriber entity.

31. (Original) A method as in claim 8 wherein registration modification transactions involve managing capabilities.

32. (Original) A method as in claim 8 wherein registration modification transactions involve cryptographic key management.

33. (Original) A method as in claim 1 further comprising:

providing, by the principal entity, at least one of a set of various service transactions to the subscriber entity.

34. (Original) A method as in claim 33 wherein said providing involves the certification of digital identities.

35. (Original) A method as in claim 33 wherein at least one of said service transactions involves assuring an entity's state.

36. (Original) A method as in claim 33 wherein at least one of said service transactions involves assuring financial information.

37. (Original) A method as in claim 33 wherein at least one of said service transactions involves assurance of identity and assurance of entity's state.

38. (Previously Presented) A method as in claim 1 wherein some of said plurality of entities are supervised by one or more other entities in at least one transaction.

39. (Previously Presented) A method as in claim 1, wherein service involves a fee based on a service agreement and contract.

40. (Previously Presented) A method as in claim 1, wherein added management and one or more additional entities assure integrity of transactions within the infrastructure.

41. (Previously Presented) A method as in claim 40 wherein integrity of the management function is enhanced by providing two or more independent reports.

42. (Original) A method as in claim 40 wherein the management function controls actions of assurance offering entities on a per transaction basis.

43. (Currently Amended) In an infrastructure in which some of a plurality of entities provide cryptographically supported services, a method of registering a subscriber entity of a plurality of entities at a principal entity of a plurality of entities, the method comprising:

a registrar entity of the plurality of entities receiving a request message from the subscriber entity requesting service from the principal entity;

the registrar entity verifying the subscriber entity and forwarding the request for service to the principal entity for storage by the principal entity; and

the registrar entity receiving from the principal entity an acknowledgement message, the acknowledgement stating acceptance and authentication/authorization information that the subscriber entity requires to obtain or access the requested service, verifying the authenticity of the received acknowledgement message, and, if correct, forwarding the acknowledgement message to the subscriber entity,

wherein the request message contains an indication of a type of service requested by the subscriber entity and contains one or more selected from the following:

(a) a unique reference to the subscriber entity;

(b) attributes about the subscriber entity;

(c) authentication information to be used to authenticate use of the service;

(d) transactional verification information;

(e) a representation by the subscriber entity agreeing to what the subscriber entity accepts;

(f) a preferred service relationship; or

(g) a subscriber entity's authenticator.

44. (Previously Presented) A method as in claim 43, wherein the service includes:

operating a cryptographically-supported transaction involving the subscriber entity, the principal entity and possibly one or more additional entities.

45. (Previously Presented) A method as in claim 43, further comprising:

moving the registration for service from the principal entity to another entity of said plurality of entities.

46. (Currently Amended) In an infrastructure in which some of a plurality of entities provide cryptographically supported services, a method of registering a subscriber entity of a plurality of entities at a principal entity of a plurality of entities, the method comprising:

the principal entity receiving from a registrar entity of the plurality of entities a forwarded request message by the subscriber entity for service from the principal entity, the request for service sent to the registrar entity by the subscriber entity and the subscriber entity being verified by the registrar entity; and

the principal entity storing the forwarded request message and transmitting an acknowledgement message, the acknowledgement stating acceptance and authentication/authorization information that the subscriber entity requires to obtain or access the requested service, to the registrar entity for verification by the registrar entity of the authenticity of the received acknowledgement message, and, if correct, forwarding the acknowledgement message by the registrar entity to the subscriber entity,

wherein the forwarded request message contains an indication of a type of service requested by the subscriber entity and contains one or more selected from the following:

(a) a unique reference to the subscriber entity;

(b) attributes about the subscriber entity;

(c) authentication information to be used to authenticate use of the service;

(d) transactional verification information;

(e) a representation by the subscriber entity agreeing to what the subscriber entity accepts;

(f) a preferred service relationship; or

(g) a subscriber entity's authenticator.

47. (Previously Presented) A method as in claim 46, wherein the service includes:

operating a cryptographically-supported transaction involving the subscriber entity, the principal entity and possibly one or more additional entities.

48. (Previously Presented) A method as in claim 46, further comprising:

moving the registration for service from the principal entity to another entity of said plurality of entities.

Reasons For Allowance

9. The following is an Examiner's statement of reasons for allowance:

None of the art of record, taken individually or combination, disclose at least the method step or system components of:

- *a registrar entity of the plurality of entities receiving a request message from the subscriber entity requesting service from the principal entity;*
- *wherein the request message contains an indication of a type of service requested by the subscriber entity and contains one or more selected from the following:*
  - *(a) a unique reference to the subscriber entity;*
  - *(b) attributes about the subscriber entity;*
  - *(c) authentication information to be used to authenticate use of the service;*
  - *(d) transactional verification information;*
  - *(e) a representation by the subscriber entity agreeing to what the subscriber entity accepts;*
  - *(f) a preferred service relationship; or*
  - *(g) a subscriber entity's authenticator.*

The closest prior art of (Mandler et al. US 5,732,400) discloses enabling on-line transactional services among sellers (principle entities) and buyers (subscriber entities) having no previous relationship with each other. Mandler accomplishes enabling on-line transactional services among sellers (principle entities) and buyers (subscriber entities) having no previous relationship with each other by providing a financial clearinghouse (register entity) between the buyer and seller. Mandler also provides another layer of authentication and security by adding a broker to interface between the buyers/sellers and the financial clearinghouse. As taught by Mandler, the functions of the clearinghouse and the broker are to insure the authenticity of the buyers/sellers and the security of the transactional services. However, Applicant has amended independent claims 1, 43, and 46 to confirm that the claims specify that one or more of the items listed may be selected, rather than one or more of each of the items listed must be selected. In claim 4 as an example, the unique reference may be, for example, item (a), or item (b), or item (c), or any combination of items (a)-(c). Mandler fails to specifically disclose this feature as claimed in the instant invention.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- O'Mahony et al. Electronic Payment Systems © 1997 ARTECH House, INC. Norwood, MA (pages 125-143) discloses electronic checks and a four party transaction system.
- Ehlert et al. (EP 0693742 A2) discloses a tariff metering system.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **571.272.6712.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

571-273-8300 [Official communications, After Final communications labeled "Box AF"]

571-273-8300 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

03 August 2006

JAMES A. REAGAN
PRIMARY EXAMINER